



# UNITED STATES PATENT AND TRADEMARK OFFICE

*MN*  
UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/075,471	02/13/2002	Jeffrey M. Ayars	109905-129462	7533

60380 7590 05/25/2007  
STEVEN C. STEWART  
REALNETWORKS, INC.  
2601 ELLIOTT AVENUE, SUITE 1000  
SEATTLE, WA 98121

EXAMINER
----------

KLIMACH, PAULA W

ART UNIT	PAPER NUMBER
----------	--------------

2135

MAIL DATE	DELIVERY MODE
-----------	---------------

05/25/2007

PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

<b>Office Action Summary</b>	Application No. 10/075,471	Applicant(s) AYARS ET AL.	
	Examiner Paula W. Klimach	Art Unit 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 19 March 2007.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-42 is/are pending in the application.
- 4a) Of the above claim(s) 34-42 is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-33 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)          | 4) <input type="checkbox"/> Interview Summary (PTO-413)           |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____                                      |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)          | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____  | 6) <input type="checkbox"/> Other: _____                          |

## **DETAILED ACTION**

### ***Response to Amendment***

This office action is in response to amendment filed on 03/19/07. The amendment filed on 03/19/07 have been entered and made of record. Therefore, presently pending claims are 1-42.

### ***Response to Arguments***

Applicant's arguments filed 03/19/07 have been fully considered. The delay in treatment of claims 34-42 is regretted. It is noted that claims 34-42 were newly added in the Amendment filed 10/16/06.

In reference to the applicant's arguments, applicant argued that the cited documents, even under Examiner's interpretation do not teach Assignee's claimed subject matter either alone or in combination. This is not found persuasive. The combination of the documents cited does indeed teach the assignee's claimed subject matter. The applicant argues further that Horstmann does not teach a plurality of modules as recited by Assignee's claimed subject matter and Assignee respectfully asserts that the remaining cited documents do not cure this deficiency. This is not found persuasive. The combination of documents, as disclosed in the rejection below, does indeed cure the deficiencies of Hortmann.

The applicant argues that the protector 103 of Horstmann does not correspond to a tamper resistant module because the tamper resistant module of the application is a tamper resistant module because the module itself is tamper resistant not because it protects content. This is not found persuasive. The definition of tamper resistant is to prevent from weakening or changing.

The system of Horstmann protects the content and therefore prevents from weakening or changing. The claim is silent as to whether the object is tamper resistant because it prevents weakening of the content or it is tamper resistant because it prevents weakening of itself.

The applicant argues that column 5 lines 54-59 does not teach a plurality of plain text digital content rendering modules communicatively coupled with each other in a hierarchical manner forming a hierarchy of modules. This is persuasive. However, Fig. 3 indicates the network card, video card and other parts of the system that are controlled in a hierarchical structure. The items are in a hierarchical structure because it is arranged in a ranked series, which is the definition of hierarchical structure. The hierarchical structure is such that the protector is the top of the hierarchy and therefore controls the systems under it. In the section of column 5 lines 54-59 indicate that the system goes down the list of protection measures. This also suggests a hierarchy because the list starts from a beginning to an end.

In addition the applicant argues that in claim 2 the examiner states that there is no root module. This is persuasive. However the examiner believes that the document (Jackson) overcomes the limitation of Horstman. Jackson discloses a method of solving an actuation allocation problem by breaking the solution into modules. This method of problem solving may be used in the system of Horstmann so that the system has a tree structure with a root module.

The applicant argues further that Jackson does not disclose teach a non-leaf module is equipped to verify the immediate downstream module as not having been compromised. This is not persuasive. The system of Jackson teaches goals sent to the root node (page 6 paragraph 0088). The goal information is received from the middle level nodes and therefore discloses when one node is not working and therefore compromised.

The applicant argues further that a compromised downstream module is not status information. However, due to connectivity of the Jackson system, the compromised node affects the rest of the system and therefore cause status (goal) information to be passed from one to another node.

The applicant argues further that a software module that receives information in no way teaches or suggests an apparatus wherein the non-leaf modules is equipped to further verify the immediate downstream module remains un-compromised before each transfer of recovered digital content to the immediate downstream module. The examiner disagrees with this argument because receiving information from a module that is downstream indicates that the module is un-compromised. In the case that the module was compromised no information would be transferred.

The applicant argued further that Hortmann does not teach or suggest an apparatus wherein a first subset of the plain text digital content rendering modules are member modules of a first application domain, and second subset of the plain text digital content rendering module are member modules of a second application domain. This is not found persuasive. As the examiner discloses below, "Hortmann discloses different methods of securing the data (column 6 lines 1-5)." The BYO suggests that the security will match the network in which the system of Hortmann is installed. As a result the result the security for a network that is separated into domains results in BYO for each domain.

In response to applicant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so

Art Unit: 2135

long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971).

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, the software system set top boxes and home media players require security to protect them and use the same type of securities.

The examiner asserts that the documents cited below do teach or suggest the subject matter broadly recited in independent Claims. Dependent Claims are also rejected at least by virtue of their dependency on independent claims and by other reason set forth in this office action.

### ***Election/Restrictions***

Claims 34-42 were newly added in the Amendment filed 10/16/06 and are directed to an invention that is independent and distinct from the invention original claims 1-33 for the following reasons:

Claims 34-42 are directed to determining that changes have been made to computer programs and therefore compromising computer programs which is classified in 713/187.

Whereas claims 1-33 are classified in 713/194 wherein a physical barrier has been provided to protect a component providing cryptographic processing a digital processing system. The system of checking for compromised computer programs has a separate utility from a tamper resist system. One system protects from tamper and the other checks when tampering has already occurred.

Since applicant has received an action on the merits for the originally presented claimed invention, this invention has been constructively elected by original presentation for prosecution on the merits. Accordingly, claim 34-42 withdrawn from consideration as being directed to a non-elected invention. See 37 CFR 1.142(b) and MPEP § 821.03.

### ***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

**Claims 1, 5-8 and 29** are rejected under 35 U.S.C. 103(a) as being unpatentable over Horstmann (6,044,469) in view of the article by M2 Presswire (“AMINO COMMUNICATIONS: Amino launches innovative approach to securing broadband communications; New technology provides digital rights protection for streaming content”) and further in view of Shear (6, 157, 721) and further in view of Jackson (2003/0002447).

*In reference to claims 1 and 29* Horstmann discloses a software publisher or distributor configurable software security mechanism (title). The apparatus disclosed by Hortmann is a

Art Unit: 2135

tamper resistant digital content recovery module wherein the tamper resistance is provided by the protection wrapper, which runs code that performs the protection options, selected by the publisher (column 5 lines 2-30). The system of Hortmann discloses a plurality of plain text digital content rendering modules communicatively coupled with each other in a hierarchical manner forming a hierarchy of modules (column 5 lines 54-59), with selective combinations of which to be selectively employed to render the recovered digital contents of corresponding types (column 6 lines 10-21), including one of the plain text digital content rendering modules occupying a root position (part 100 Fig. 5) of the hierarchy to exclusively receive the recovered digital contents to be rendered, of all types, from the tamper resistant digital content recovery module (column 6 lines 10-26). The system of Horstman includes one or more storage units to store said tamper resistant module and said plurality of plain text digital content rendering modules (column 6 lines 5-10); and a processor coupled with the one or more storage units to execute the tamper resistant module and the plurality of plain text digital content rendering modules (column 6 lines 6-22).

Although Horstman discloses recovering protected digital contents, Horstman does not expressly disclose a system to recover protected digital contents of various types in an obfuscated manner.

The article by the M2 Presswire discloses a system that varies the level of encryption in real time depending upon the type and value of content or transaction. Therefore the system recovers protected digital contents in an obfuscated manner and the digital content is of various types (Full Text paragraphs 2-3).



At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to recover protected digital contents of various types in an obfuscated manner as disclosed by the article by M2 Presswire in the system of Horstman. One of ordinary skill in the art would have been motivated to do this because combining proven techniques minimizes the risk to content dynamically without compromising performance.

Although Horstman discloses rendering plain text, Horstmann does not disclose the digital content as defined by the applicant (multimedia digital content).

Shear discloses a system with tamper resistant work factors to protect itself from load modules (abstract). Shear discloses loading modules for computers and set top boxes and therefore the rendering module for multimedia (column 18 lines 45-67). The system of Shear discloses a load module for movies as well as software (column 8 lines 40-56).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the loading module that is tamper resistant as in Shear in the system of Horstmann. One of ordinary skill in the art would have been motivated to do this because defective, bogus and unauthorized computer information can wreak havoc within an electronic system (column 8 lines 14-19).

Although Horstman discloses a content rendering module, Horstman and Gruanke do not disclose root module.

Jackson teaches an apparatus and methods that approximately solve an actuation allocation problem by breaking the solution into modules (abstract). The root in the system of Jackson includes the parts 135 and 191 on Figure 1. Jackson further teaches multiple modules.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use a hierarchical system wherein there is a root and nodes as in Jackson in the system of Hortmann. One of ordinary skill in the art would have been motivated to do this because it enables the system to break down the problem into smaller problems that can be solved in an optimal way or by breaking the smaller allocation problem down into yet smaller problems (page 1 paragraph 0017).

*In reference to claim 8*, neither Horstmann nor the M2 presswire disclose a system wherein the non-leaf modules is equipped to verify the immediate downstream module as not having been compromised by verifying a signature of the immediate downstream module.

Shear discloses a system wherein the non-leaf modules is equipped to verify the immediate downstream module as not having been compromised by verifying a signature of the immediate downstream module (column 14 lines 49-60).

*In reference to claim 5*, neither Horstmann nor the M2 presswire article disclose a system wherein the hierarchy of modules includes a module occupying a non-leaf position in the hierarchy and a module occupying an immediate downstream position in the hierarchy from the non-leaf plain text digital content rendering module, and the non-leaf modules is equipped to verify the immediate downstream module as not having been compromised.

Shear discloses a system wherein the hierarchy of modules includes a module occupying a non-leaf position in the hierarchy and a module occupying an immediate downstream position in the hierarchy from the non-leaf plain text digital content rendering module, and the non-leaf modules is equipped to verify the immediate downstream module as not having been compromised (column 6 lines 16-33).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the loading module that is tamper resistant as in Shear in the system of Horstmann. One of ordinary skill in the art would have been motivated to do this because defective, bogus and unauthorized computer information can wreak havoc within an electronic system (column 8 lines 14-19).

Horstmann, M2 presswire and Shear do not disclose the non-leaf module is equipped to verify the immediate downstream module as not having been compromised.

Jackson discloses the controller that is the root and therefore a non-leaf module receives the current status (goal) information (page 6 paragraph 0088).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use a hierarchical system wherein there is a root and nodes as in Jackson in the system of Hortmann. One of ordinary skill in the art would have been motivated to do this because it enables the system to break down the problem into smaller problems that can be solved in an optimal way or by breaking the smaller allocation problem down into yet smaller problems (page 1 paragraph 0017).

*In reference to claim 6*, neither Horstmann nor the M2 presswire disclose a system wherein the non-leaf modules is equipped to verify the immediate downstream module not having been compromised at least during initialization.

Shear discloses a system wherein the non-leaf modules is equipped to verify the immediate downstream module not having been compromised at least during initialization (column 6 lines 16-33).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the loading module that is tamper resistant as in Shear in the system of Horstmann. One of ordinary skill in the art would have been motivated to do this because defective, bogus and unauthorized computer information can wreak havoc within an electronic system (column 8 lines 14-19).

Horstmann, M2 presswire and Shear do not disclose the non-leaf module is equipped to verify the immediate downstream module as not having been compromised. Wherein a compromised downstream module is status information.

Jackson discloses the controller that is the root and therefore a non-leaf module receives the current status information (page 3 paragraph 0045). Wherein a compromised downstream module is status information.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use a hierarchical system wherein there is a root and nodes as in Jackson in the system of Hortmann. One of ordinary skill in the art would have been motivated to do this because it enables the system to break down the problem into smaller problems that can be solved in an optimal way or by breaking the smaller allocation problem down into yet smaller problems (page 1 paragraph 0017).

*In reference to claim 7*, neither Horstmann nor the M2 presswire disclose a system wherein the non-leaf modules is equipped to further verify the immediate downstream module remains uncompromised before each transfer of recovered digital content to the immediate downstream module.

Art Unit: 2135

Shear discloses a system wherein the non-leaf modules is equipped to further verify the immediate downstream module remains uncompromised before each transfer of recovered digital content to the immediate downstream module.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the loading module that is tamper resistant as in Shear in the system of Horstmann. One of ordinary skill in the art would have been motivated to do this because defective, bogus and unauthorized computer information can wreak havoc within an electronic system (column 8 lines 14-19).

Horstmann, M2 presswire and Shear do not disclose the non-leaf module is equipped to verify the immediate downstream module as not having been compromised. Wherein a compromised downstream module is status information.

Jackson discloses the controller that is the root and therefore a non-leaf module receives the current status information (page 3 paragraph 0045). Wherein a compromised downstream module is status information.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use a hierarchical system wherein there is a root and nodes as in Jackson in the system of Hortmann. One of ordinary skill in the art would have been motivated to do this because it enables the system to break down the problem into smaller problems that can be solved in an optimal way or by breaking the smaller allocation problem down into yet smaller problems (page 1 paragraph 0017).

**Claims 2, 11, 24, and 30** are rejected under 35 U.S.C. 103(a) as being unpatentable over Horstmann in view of the article by M2 Presswire and further in view of Shear, and further in view of Jackson as applied to claims 1 and 29 above, and further in view of Graunke et al (5, 991, 399).

*In reference to claims 2 and 30* Horstman discloses the tamper resistant digital content recovery module with a root one of the plurality of hierarchically organized plain text digital content rendering module; however Horstman does not disclose verifying the module has not been compromised. Horstman further does not disclose the root verifying an immediate downstream module is uncompromised before transferring the first digital content to the immediate downstream module to further the rendering of the first digital content.

Grauke discloses a method for securely distributing a conditional use private key to a trusted entity on a remote system (abstract). The system of Graunke determines if the system is a trust worthy player (software) before providing the user with the key and therefore access to digital content (column 3 line 53 to column 4 line 7). In the case that the player is compromised the player does not have the ability to perform the cryptographic operation (column 4 lines 7-14).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add the check for a trusted (compromised integrity) player and not allow access to digital content based on the verification of the software (module) as in Graunke in the system of Horstman. One of ordinary skill in the art would have been motivated to do this because the integrity of the trusted player is correlated to its ability to perform a cryptographic operation

using an asymmetric key pair in a manner that is tamper resistant thereby preventing an unencrypted copy of digital content to be made (abstract).

Although Horstman discloses a content rendering module, Horstman and Gruanke do not disclose root module.

Jackson teaches an apparatus and methods that approximately solve an actuation allocation problem by breaking the solution into modules (abstract). The root in the system of Jackson includes the parts 135 and 191 on Figure 1.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use a hierarchical system wherein there is a root and nodes as in Jackson in the system of Hortmann. One of ordinary skill in the art would have been motivated to do this because it enables the system to break down the problem into smaller problems that can be solved in an optimal way or by breaking the smaller allocation problem down into yet smaller problems (page 1 paragraph 0017).

*In reference to claims 11 and 24* wherein a first subset of the plain text digital content rendering modules are member modules of a first application domain, and a second subset of the plain text digital content rendering modules are member modules of a second application domain. Horstmann discloses different methods of securing the data (column 6 lines 1-5). Therefore at the time the invention was made, it would have been obvious to a person of ordinary skill in the art to also render modules are member modules of a second application domain. One of ordinary skill in the art would have been motivated to do this because dividing modules by domain is an easy and convenient method of organizing information.

**Claims 3-4, 9-10, 12-23, 25-28 and 31-33** are rejected under 35 U.S.C. 103(a) as being unpatentable over Horstmann, in view of the article by M2 Presswire, further in view of Shear, and further in view of Jackson as applied to claims 1 and 29 above, and further in view of Graunke et al (5, 991, 399).

*In reference to claim 12*, Horstmann discloses a software publisher or distributor configurable software security mechanism (title). The system comprises a root one of a plurality of hierarchically organized plain text digital content rendering modules collectively equipped to render digital contents requesting a tamper resistant digital content recovery module to recover a first protected digital content (column 5 lines 54-59). The tamper resistant digital content recovery module recovering the first protected digital content (part 100 Fig. 5), and transferring the recovered first digital content to said root one of the plurality of hierarchically organized plain text digital content rendering modules (column 6 lines 10-21), and said root one in conjunction with first at least one other one of said plurality of hierarchically organized digital content rendering modules rendering said first digital content (column 6 lines 10-21),

Although Horstman discloses recovering protected digital contents, Horstman does not expressly disclose a system to recover protected digital contents of various types in an obfuscated manner.

The article by the M2 Presswire discloses a system that varies the level of encryption in real time depending upon the type and value of content or transaction. Therefore the system recovers protected digital contents in an obfuscated manner and the digital content is of various types (Full Text paragraphs 2-3).



At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to recover protected digital contents of various types in an obfuscated manner as disclosed by the article by M2 Presswire in the system of Horstman. One of ordinary skill in the art would have been motivated to do this because combining proven techniques minimizes the risk to content dynamically without compromising performance.

Horstman discloses the tamper resistant digital content recovery module with a root one of the plurality of hierarchically organized plain text digital content rendering module; however Horstman does not disclose verifying the module has not been compromised. Although the claim recites, "...rendering modules has not been comprised..." the examiner assumes that the applicant meant compromised. Horstman further does not disclose the root verifying an immediate downstream module is uncompromised before transferring the first digital content to the immediate downstream module to further the rendering of the first digital content.

Grauke discloses a method for securely distributing a conditional use private key to a trusted entity on a remote system (abstract). The system of Graunke determines if the system is a trust worthy player (software) before providing the user with the key and therefore access to digital content (column 3 line 53 to column 4 line 7). In the case that the player is compromised the player does not have the ability to perform the cryptographic operation (column 4 lines 7-14).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add the check for a trusted (compromised integrity) player and not allow access to digital content based on the verification of the software (module) as in Graunke in the system of Horstman. One of ordinary skill in the art would have been motivated to do this because the integrity of the trusted player is correlated to its ability to perform a cryptographic operation

using an asymmetric key pair in a manner that is tamper resistant thereby preventing an unencrypted copy of digital content to be made (abstract).

*In reference to claims 18 and 25* Horstmann discloses a software publisher or distributor configurable software security mechanism (title). The apparatus disclosed by Hortmann is a tamper resistant digital content recovery module wherein the tamper resistance is provided by the protection wrapper, which runs code that performs the protection options, selected by the publisher (column 5 lines 2-30). The system of Hortmann discloses a plurality of plain text digital content rendering modules communicately coupled with each other in a hierarchical manner forming a hierarchy of modules (column 5 lines 54-59), with selective combinations of which to be selectively employed to render the recovered digital contents of corresponding types (column 6 lines 10-21), including one of the plain text digital content rendering modules occupying a root position (part 100 Fig. 5) of the hierarchy to exclusively receive the recovered digital contents to be rendered, of all types, from the tamper resistant digital content recovery module (column 6 lines 10-26). The system of Horstman includes one or more storage units to store said tamper resistant module and said plurality of plain text digital content rendering modules (column 6 lines 5-10); and a processor coupled with the one or more storage units to execute the tamper resistant module and the plurality of plain text digital content rendering modules (column 6 lines 6-22).

Although Horstman discloses recovering protected digital contents, Horstman does not expressly disclose a system to recover protected digital contents of various types in an obfuscated manner.

The article by the M2 Presswire discloses a system that varies the level of encryption in real time depending upon the type and value of content or transaction. Therefore the system recovers protected digital contents in an obfuscated manner and the digital content is of various types (Full Text paragraphs 2-3).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to recover protected digital contents of various types in an obfuscated manner as disclosed by the article by M2 Presswire in the system of Horstman. One of ordinary skill in the art would have been motivated to do this because combining proven techniques minimizes the risk to content dynamically without compromising performance.

Horstman discloses the tamper resistant digital content recovery module with a root one of the plurality of hierarchically organized plain text digital content rendering module; however Horstman does not disclose verifying the module has not been compromised. Horstman further does not disclose the root verifying an immediate downstream module is uncompromised before transferring the first digital content to the immediate downstream module to further the rendering of the first digital content.

Grauke discloses a method for securely distributing a conditional use private key to a trusted entity on a remote system (abstract). The system of Graunke determines if the system is a trust worthy player (software) before providing the user with the key and therefore access to digital content (column 3 line 53 to column 4 line 7). In the case that the player is compromised the player does not have the ability to perform the cryptographic operation (column 4 lines 7-14).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add the check for a trusted (compromised integrity) player and not allow access to digital content based on the verification of the software (module) as in Graunke in the system of Horstman. One of ordinary skill in the art would have been motivated to do this because the integrity of the trusted player is correlated to its ability to perform a cryptographic operation using an asymmetric key pair in a manner that is tamper resistant thereby preventing an unencrypted copy of digital content to be made (abstract).

*In reference to claims 3 and 19-20* Horstman discloses the tamper resistant digital content recovery module with a root one of the plurality of hierarchically organized plain text digital content rendering module; however Horstman does not disclose verifying the content rendering module.

Grauke discloses a method for securely distributing a conditional use private key to a trusted entity on a remote system (abstract). The system of Graunke determines if the system is a trust worthy player (software) before providing the user with the key and therefore access to digital content (column 3 line 53 to column 4 line 7). The system of Graunke includes a tamper resistant module is equipped to verify the plain text digital content rendering module (Fig. 2). The verification of the module is in response to request from the tamper resistant module (column 4 lines 5-7).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add the check for a trusted (compromised integrity) player and not allow access to digital content based on the verification of the software (module) as in Graunke in the system of Horstman. One of ordinary skill in the art would have been motivated to do this because the

Art Unit: 2135

integrity of the trusted player is correlated to its ability to perform a cryptographic operation using an asymmetric key pair in a manner that is tamper resistant thereby preventing an unencrypted copy of digital content to be made (abstract).

*In reference to claims 4, 13-15, 21, 26, and 31* Horstman discloses the tamper resistant digital content recovery module with a root one of the plurality of hierarchically organized plain text digital content rendering module; however Horstman does not disclose verifying the content rendering module.

Grauke discloses a method wherein the tamper resistant module is equipped to verify the plain text digital content rendering module occupying the root position of the hierarchy by verifying a signature of the plain text digital content rendering module occupying the root position.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add the check for a trusted (compromised integrity) player and not allow access to digital content based on the verification of the software (module) as in Graunke in the system of Horstman. One of ordinary skill in the art would have been motivated to do this because the integrity of the trusted player is correlated to its ability to perform a cryptographic operation using an asymmetric key pair in a manner that is tamper resistant thereby preventing an unencrypted copy of digital content to be made (abstract).

*In reference to claims 8, 22, and 32*, wherein the digital content of various types comprises streaming media contents of a plurality of media, and of a plurality of format types.

Art Unit: 2135

The article by the M2 Presswire discloses a system that varies the level of encryption in real time depending upon the type and value of content or transaction. Therefore the system recovers protected digital contents in an obfuscated manner and the digital content is of various types (Full Text paragraphs 2-3). The digital content disclosed includes all types of multimedia, for data, video , audio, news feeds and web pages (Full Text paragraphs 2).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to recover protected digital contents of various types in an obfuscated manner as disclosed by the article by M2 Presswire in the system of Horstman. One of ordinary skill in the art would have been motivated to do this because combining proven techniques minimizes the risk to content dynamically without compromising performance.

*In reference to claims 10 and 23* wherein the apparatus is a selected one of a wireless mobile phone, a palm sized personal digital assistant, a notebook computer, a set-top box, a desktop computer, a single processor server, a multi-processor server, and a cluster of coupled systems (column 5 lines 1-7).

*In reference to claim 33* wherein the recordable medium is a selected one of a magnetically recordable medium and an optically recordable medium.

*In reference to claims 16 and 28* wherein the method further comprises the root one of the plurality of hierarchically organized plain text digital content rendering modules requesting the tamper resistant digital content recovery module to recover a second protected digital content of the same first type; the tamper resistant digital content recovery module verifying that said root one of the plurality of hierarchically organized plain text digital content rendering modules

has not been comprised; the tamper resistant digital content recovery module recovering the second protected digital content in an obfuscated manner, and transferring the recovered second digital content to said root one of the plurality of hierarchically organized plain text digital content rendering modules; and said root one in conjunction with the same first at least one other one of said plurality of hierarchically organized digital content rendering modules rendering said second digital content, with each of said root and same non-leaf ones, if any, of said first at least one other one of said plurality of hierarchically organized digital content rendering modules verifying an immediate downstream module is uncompromised before transferring the second digital content to the immediate downstream module to further the rendering of the second digital content.

Horstman discloses a system with the root one of the plurality of hierarchically organized plain text digital content rendering modules requesting the tamper resistant digital content recovery module (Fig. 5). The system is used to recover digital content and therefore recovers a second protected digital content of the same first type. The tamper resistant digital content recovery module recovering the second protected digital content in an obfuscated manner, and transferring the recovered second digital content to said root one of the plurality of hierarchically organized plain text digital content rendering modules (column 6 lines 10-22). Wherein the protected digital content is transferred to protector, which then runs the code selected using the software protection parameters.

Horstman discloses the tamper resistant digital content recovery module with a root one of the plurality of hierarchically organized plain text digital content rendering module; however Horstman does not disclose verifying the module has not been compromised. Horstman further

Art Unit: 2135

does not disclose the root verifying an immediate downstream module is uncompromised before transferring the first digital content to the immediate downstream module to further the rendering of the first digital content.

Grauke discloses a method for securely distributing a conditional use private key to a trusted entity on a remote system (abstract). The system of Graunke determines if the system is a trust worthy player (software) before providing the user with the key and therefore access to digital content (column 3 line 53 to column 4 line 7). In the case that the player is compromised the player does not have the ability to perform the cryptographic operation (column 4 lines 7-14).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add the check for a trusted (compromised integrity) player and not allow access to digital content based on the verification of the software (module) as in Graunke in the system of Horstman. One of ordinary skill in the art would have been motivated to do this because the integrity of the trusted player is correlated to its ability to perform a cryptographic operation using an asymmetric key pair in a manner that is tamper resistant thereby preventing an unencrypted copy of digital content to be made (abstract).

*In reference to claims 17 and 27* wherein the method further comprises the root one of the plurality of hierarchically organized plain text digital content rendering modules requesting the tamper resistant digital content recovery module to recover a second protected digital content of the same first type; the tamper resistant digital content recovery module verifying that said root one of the plurality of hierarchically organized plain text digital content rendering modules has not been comprised; the tamper resistant digital content recovery module recovering the



second protected digital content in an obfuscated manner, and transferring the recovered second digital content to said root one of the plurality of hierarchically organized plain text digital content rendering modules; and said root one in conjunction with the same first at least one other one of said plurality of hierarchically organized digital content rendering modules rendering said second digital content, with each of said root and same non-leaf ones, if any, of said first at least one other one of said plurality of hierarchically organized digital content rendering modules verifying an immediate downstream module is uncompromised before transferring the second digital content to the immediate downstream module to further the rendering of the second digital content.

Horstman discloses a system with the root one of the plurality of hierarchically organized plain text digital content rendering modules requesting the tamper resistant digital content recovery module (Fig. 5). The system is used to recover digital content and therefore recovers a second protected digital content of the same first type. The tamper resistant digital content recovery module recovering the second protected digital content in an obfuscated manner, and transferring the recovered second digital content to said root one of the plurality of hierarchically organized plain text digital content rendering modules (column 6 lines 10-22). Wherein the protected digital content is transferred to protector, which then runs the code selected using the software protection parameters.

Horstman discloses the tamper resistant digital content recovery module with a root one of the plurality of hierarchically organized plain text digital content rendering module; however Horstman does not disclose verifying the module has not been compromised. Horstman further does not disclose the root verifying an immediate downstream module is uncompromised before

Art Unit: 2135

transferring the first digital content to the immediate downstream module to further the rendering of the first digital content.

Grauke discloses a method for securely distributing a conditional use private key to a trusted entity on a remote system (abstract). The system of Graunke determines if the system is a trust worthy player (software) before providing the user with the key and therefore access to digital content (column 3 line 53 to column 4 line 7). In the case that the player is compromised the player does not have the ability to perform the cryptographic operation (column 4 lines 7-14).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add the check for a trusted (compromised integrity) player and not allow access to digital content based on the verification of the software (module) as in Graunke of the root module and the leaf modules of the system of Horstman. One of ordinary skill in the art would have been motivated to do this because the integrity of the trusted player is correlated to its ability to perform a cryptographic operation using an asymmetric key pair in a manner that is tamper resistant thereby preventing an unencrypted copy of digital content to be made (abstract).

### ***Conclusion***

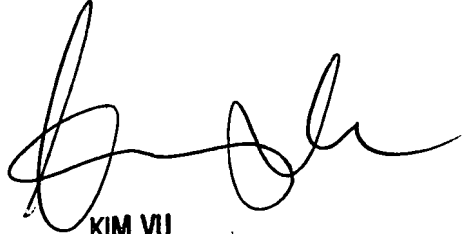
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W. Klimach whose telephone number is (571) 272-3854. The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

Art Unit: 2135

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PWK  
Thursday, May 24, 2007



**KIM VU**  
**SUPERVISORY PATENT EXAMINER**  
**TECHNOLOGY CENTER 2**